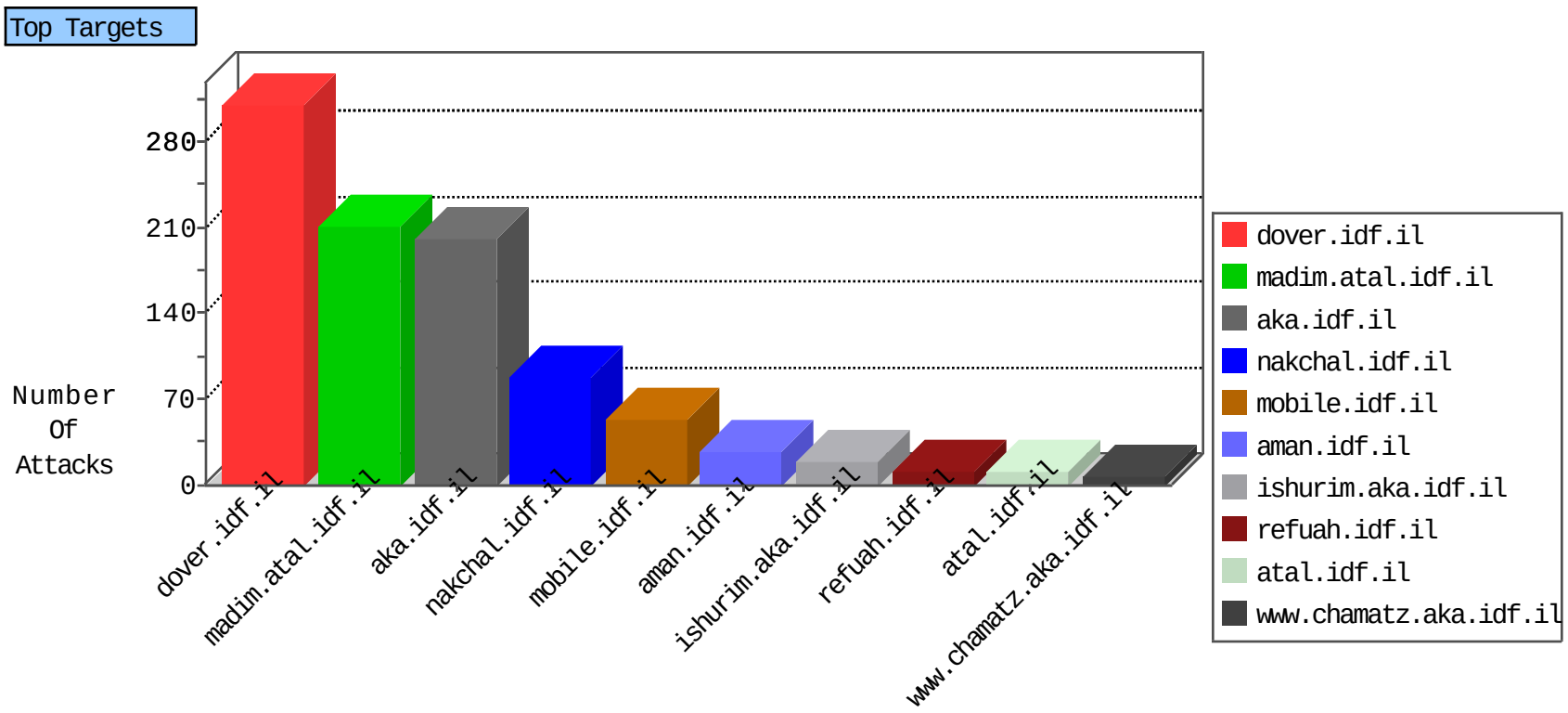
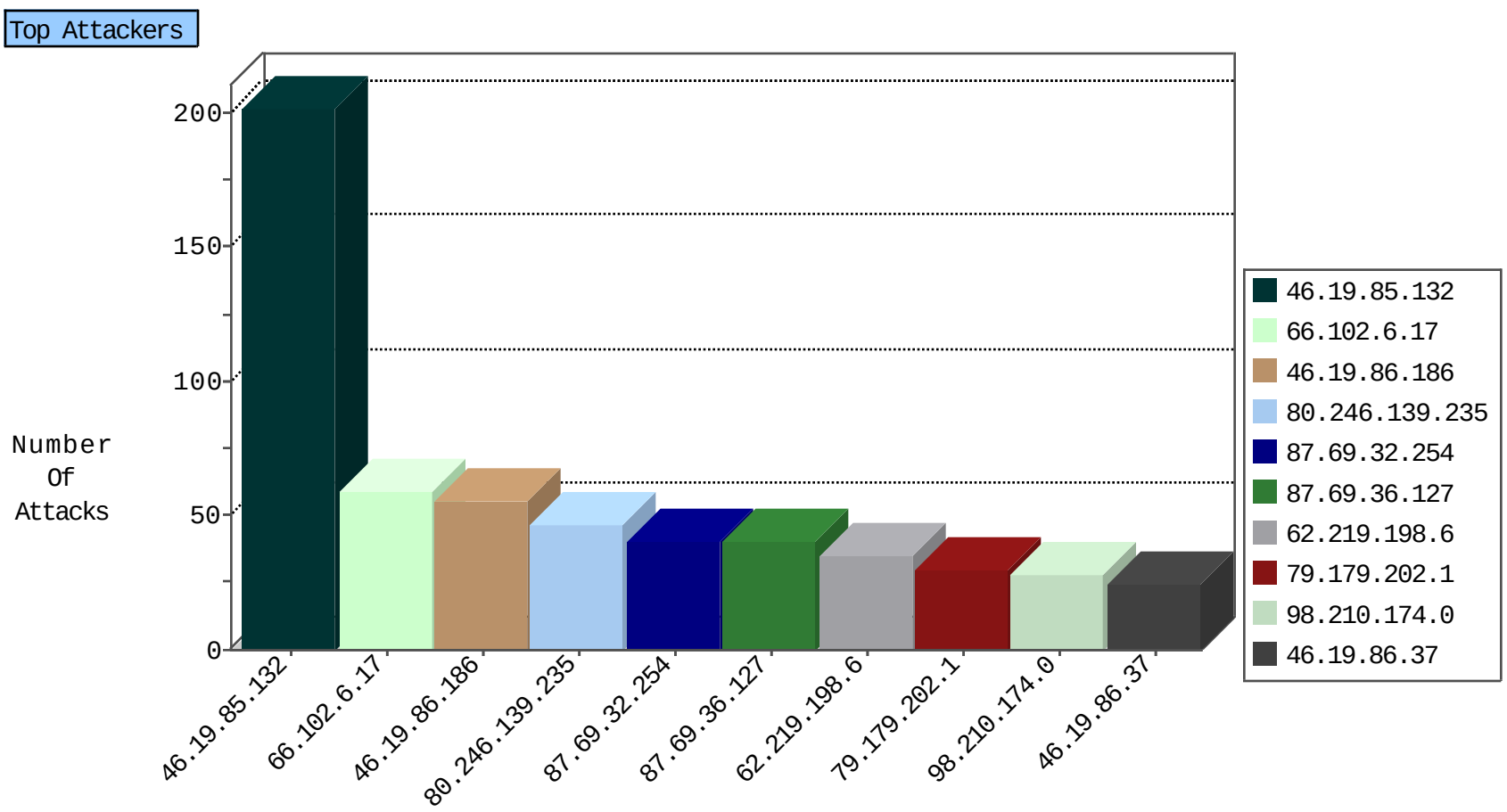
09-19-2016-19:04:02 to 09-19-2016-20:04:02

IDF Under Attack
Daily Report





09-19-2016-19:04:02 to 09-19-2016-20:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
141.226.161.121	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
128.208.4.197	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.133.224.147	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
129.97.74.14	Canada	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
194.29.178.14	Poland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.139	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-19-2016-19:04:02 to 09-19-2016-20:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-19-2016-19:04:02 to 09-19-2016-20:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.102.6.17	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	57
139.215.201.243	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
45.63.116.255	147.237.76.44	Germany	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
200.98.129.133	147.237.77.176	Brazil	matpash.idf.il	ET SCAN Potential SSH Scan	1
43.245.183.109	147.237.8.50	Indonesia	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
200.98.129.133	147.237.72.156	Brazil	aman.idf.il	ET SCAN Potential SSH Scan	1
23.92.20.154	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.129.15	147.237.0.17	United Kingdom	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
139.162.168.200	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
108.61.188.59	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.76.30	Ukraine	himush.idf.il	ET SCAN NMAP -sS window 3072	1
74.63.237.154	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
219.146.251.139	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
43.245.183.109	147.237.8.50	Indonesia	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
200.98.129.133	147.237.77.61	Brazil	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
23.239.31.132	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.129.15	147.237.77.19	United Kingdom	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
2.55.38.47	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
139.162.168.200	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.201.236.155	147.237.76.30	Ukraine	himush.idf.il	ET SCAN NMAP -sS window 4096	1
77.138.230.68	147.237.77.233	France	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
69.162.69.222	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	1

09-19-2016-19:04:02 to 09-19-2016-20:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.179.202.1	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
87.69.36.127	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	23
87.69.32.254	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
87.69.32.254	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
80.246.139.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
87.69.36.127	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
98.210.174.0	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
98.210.174.0	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
80.246.139.235	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
2.53.172.19	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.242	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
80.246.139.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.186	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	11
46.19.86.186	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
46.19.86.186	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
37.105.240.43	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
62.219.198.6	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
46.19.86.186	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
46.19.86.37	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.19.86.186	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
5.102.195.73	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.55.10.151	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
109.253.156.47	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.147.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.251	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.114.5.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.55.38.246	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.186	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.19.86.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
82.205.81.223	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
176.13.235.178	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
212.235.16.21	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
100.92.180.208		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
79.181.249.132	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
131.253.25.179	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.53.135.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
87.69.206.200	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
87.69.206.200	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
141.226.217.130	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
98.230.26.29	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
212.235.16.21	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.86.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
87.69.206.200	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.120.45.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.37	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
77.139.212.21	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
37.26.148.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

09-19-2016-19:04:02 to 09-19-2016-20:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	200
62.219.198.6	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	14
62.219.198.6	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 62.219.198.6	Block	12
109.64.194.130	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	11
80.246.139.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
37.26.147.220	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/1.he/infocenteritem/	Block	2
77.125.88.4	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
109.64.194.130	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 109.64.194.130	Block	2
2.55.38.246	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
40.77.167.33	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	2
77.138.16.110	France	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.138.128.113	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	2
31.210.186.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
192.116.2.47	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
2.53.161.163	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
77.139.38.209	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
62.219.198.6	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	1
147.236.232.252	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
84.109.72.73	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.109.72.73	Block	1
46.19.85.132	Israel	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Open Mode	None	1
197.89.111.179	South Africa	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/	Block	1
2.55.38.246	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.139.174.62	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
37.46.38.172	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
148.251.176.212	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 148.251.176.212	Block	1
84.109.72.73	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	1
77.126.45.21	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl75 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.19.85.132	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/mobile/templates/basket/basket.aspx	Block	1
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
109.64.194.130	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/8/	Block	1
68.180.229.223	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
148.251.176.212	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/home/default.aspx	Block	1
85.64.225.17	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Open Mode	None	1
213.57.183.183	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/www.tikshuv.idf.il	Block	1
109.253.135.156	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout.css	Block	1
2.55.143.155	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
82.34.78.113	United Kingdom	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
68.180.229.223	United States	147.237.77.216	dover.idf.il	Parameter Type Violation aspxerrorpath in www.idf.il/error.htm	Block	1
46.19.85.121	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	1
178.252.94.5	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
87.69.122.69	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1273-he/atal.aspx	Block	1
2.53.24.191	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
217.69.133.245	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/jeninkilled/stn	Block	1
109.253.156.47	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
82.81.63.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.125.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1

09-19-2016-19:04:02 to 09-19-2016-20:04:02